IAPTC 26th Annual Conference

Peace Operations in the Digital Era – Opportunities and Challenges for the Global Training Community

Opportunities and challenges identified by PKTI – Police perspective

The participation in Peace Operations often compels Police commanders to adopt decisions on particularly complex situations characterized by composite environments, sometimes chaotic, frequently requiring immediate responses. In this framework digital transformation turns out to be quintessential to ensure the highest standards of performance and sound implementation of the mandate.

The field of peacekeeping is facing upheaval, overcoming new challenges, concerning the ability to analyze large amounts of data on conflict or destabilized situations; mitigate the information risks that follow; ensure accountability and preserve public trust in an era of asymmetric security threats.

The emergence of technologies such as Artificial Intelligence techniques requires peacekeeping to anticipate new challenges in cyberspace, to improve the security of peacekeepers, as well as of the civilian populations.

During the COVID-19 pandemic, internet use has increased by 40%, so it is time to protect cyberspace, as evidenced by the Report of the Secretary-General to the General Assembly A/74/821, the "*Road map for digital cooperation*". In this context, raising sensitivity and awareness to cybersecurity issues becomes an enabler for achieving the objectives set also in Peace Operations settings where the United Nations Police are fully supporting the implementation of the Digital Transformation Strategy.

Comment [BGP(B1]: Tratto dal discoscor
introduttivo del SG allo UN COPS)

The data represents the core United Nations 2.0 model, as defined in the Report "*Our Common Agenda*" of the United Nations Secretary-General, the quintet for the change includes: "*data, analytics and communications; innovation and digital transformation; strategic foresight; behavioral science; and performance and results orientation*".

Enhanced cyber security capabilities will likely be required by missions and UNPOL will be part of those expected to use and maintain them.

As recommended in a recent study, UNPOL will need to be conversant and operational in a range of new technology, and namely in cyber capability, to effectively operate in the conflict theatres of tomorrow. Ability to use and confront new non-lethal weapons technologies will likely become important for police. Seemingly, important will be being able to use machine assistance to overcome logistics challenges and produce more on site such as equipment for local police using 3D printing. Another key area for up-skilling on new technology and techniques relates to cybercrime and security techniques. As a minimum, skill-sets around modern cyberspace intelligence gathering techniques and software familiarity will be necessary. Being able to navigate information landscapes typified by misinformation will also be essential for:

- accurate and timely conflict and crime analysis to guide responses; and;
- informing force protection in situations where peacekeepers are targeted.

Forensic cyber security capabilities will likely be required by missions and UNPOL will be part of those expected to use and maintain them. Protecting encrypted mission databases that include sensitive against attacks by malicious state and non-state actors will be critical to the effectiveness and credibility of future missions. Related, where UNPOL are engaged in capacity-building with national police, it is likely they will need to transfer the know-how to tackle cybercrime that may target critical infrastructure and systems that underwrite stability in society. DPO should look to build collaborative relationships between UNPD and existing UN capacities such as the "Digital Blue Helmets" unit in the Office of Information and Communications Technology to enhance cybersecurity preparedness, resilience and response. In fact, although there are several critical issues regarding the deployment of a full-fledged cyber peacekeeping force, this concept can be integrated into the current UN peacekeeping organizational structure as a solution to distinctly address the cyber component of future conflicts in crisis areas.

The UN new *Digital Transformation Strategy for Peacekeeping* shows the need for a data-driven approach, especially given the increasing amount of data from the proliferation of Internet access and smartphone usage in the countries of deployment of peace operations, which have caused a technology-driven transformation of the operational environment.

All this together with significant developments in the fields of artificial intelligence and machine learning, whose applications are based on huge amounts of data and which have produced some promising initiatives for UN operations.

For example, MINUSMA in Mali uses machine learning to detect hate-speeches in radio data in order to alert for potential unrest, and MONUSCO in Congo uses social media monitoring and artificial intelligence in order to detect the mission's perception of the population.

The potential of artificial intelligence tools also lies in supporting peacekeeping in conflict prediction, as demonstrated by several studies, in order to understand conflict dynamics and be able to design missions better suited to prevent the re-emergence of new conflicts.

Analytics through machine learning can also improve prevention capabilities by limiting difficulties in starting a mission, or by allowing for smarter allocation of resources.

Advances in *Natural Language Processing* are tools for translation and interpretation, improving interoperability in multinational missions and facilitating communication with the local population. In addition, the ability to process language also offers tools to analyze open-source information from social media.

This access to unprecedented amounts and types of information can provide peace operations and special political missions with a better understanding of the environment and, furthermore, a smarter emergency response, based on a decision-making process as part of the Intelligence cycle.

The UN is aware of the potential benefits and is making efforts to make the most of these new technologies. A clear example of this are the *Joint Mission Analysis Centers* (JMACS) which aim at a more integrated and predictive data-driven approach to peacekeeping with detailed reports. However, the shift from "exploring" and "raising awareness" to "regulating" and "committing resources" at the systemic level has yet to take place.

The focus shall be on a human rights based approach, at the center of all the United Nations' digital integration policies. An inclusive and gender-sensitive approach must be promoted also in the use of new technological tools, contributing to the definition of shared standards that protect human rights and strengthen local ecosystems.

For the safe dissemination and use of the new potential offered by cyberspace, it is necessary to limit the sources of risks. The greatest risk in the use of the new technology comes from human error, which is present in more than 90% of cybersecurity breaches.

The repercussions of errors in security procedures often cause enormous damage to organizations victims of cyber attacks. This entails the paramount importance of trainig and education in the digital transformation domain. The enhanced awareness allows users to learn how to behave in cyberspace, how to protect themselves from potential threats, and, consequently, protect the mission by raising the level of security.

The training of digital awareness takes place through courses to learn the principles of cybersecurity and Training Centers for personnel to be deployed in peace operations and special political missions under the aegis of the United Nations cannot ignore the provision, in the training packages, of the key elements of cybersecurity and cyberhyigiene practices. CoESPU, for instance, has substantially increased the hours of training on this topic.

Also the learning based on simulation, making resort to Command Posts such as "MaGISTrA" (*Modeling and Gaming Information Simulation Training Area*), is particularly effective. Specific programs aimed at the automation of exercises and management of dynamic of events and injections of the MEL/MIL (*Main Event List/Main Incidents List*) lists is an extremely useful tool. To this day, there are, regrettably, very few software that are able to faithfully recreate the reality of a sound post conflict situation appropriate to exercise police peacekeepers. The majority is limited to recreating simplistic visions of conflicts where the role player is limited to participating following the attack-defense dichotomy, without having to care about the legitimacy principles, legal coverage, proportionality of the use of force or simply moral consequences. To this regard, capitalizing on the current information technology knowledge, in order to recreate the multifaceted dynamics of a peace mission, or alternative scenarios that are yet to be determined and can get activated by the player's choices, would reach tangible and concrete results and the expectation of training and involvement for the audience would be a lot higher compared to, for example, the ordinary frontal lecture. Gaming could actually constitute the added value of the police training sector: both from an educational and training point of view and from an academic one.

I therefore conclude affirming that technology applied to practical training and the information technology's evolution in the sector can significantly contribute and refine the training of police peacekeepers and represent a useful and stimulating resource to improve team work, sense of belonging and cohesion as well as cybersecurity awareness and effective cyberhygene practices

DECIDEDLY MINIMIZE THE CYBER THREATS, ENHANCING THE SECURITY OF THE MISSION.

THANK YOU!